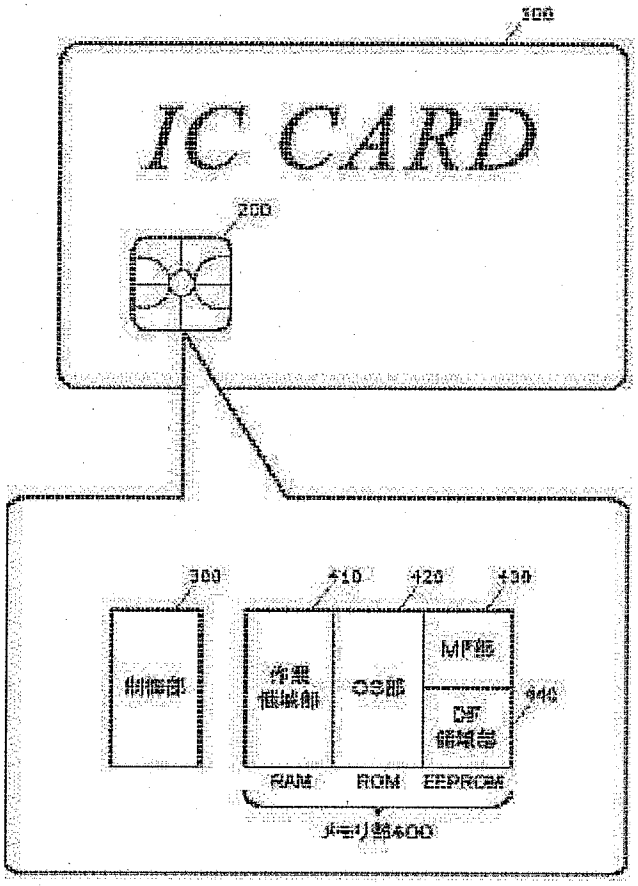
# DEVICE AND METHOD FOR CONTROLLING PROGRAM AND PROGRAM

**Publication number:** JP2002351567 (A)
**Publication date:** 2002-12-06
**Inventor(s):** NANAO SHINJI; TAKEUCHI TAKASHI; ICHIHARA NAOHISA; YAMAMOTO SHINYA
**Applicant(s):** NTT DATA CORP
**Classification:**
**- international:** ***B42D15/10; G06F1/00; G06F21/22; G06K19/073;*** **B42D15/10; G06F1/00; G06F21/22; G06K19/073;** (IPC1-7): G06F1/00; B42D15/10; G06K19/073
**- European:**
**Application number:** JP20010159183 20010528
**Priority number(s):** JP20010159183 20010528

**Also published as:**
JP4028697 (B2)

Abstract of **JP 2002351567 (A)**

PROBLEM TO BE SOLVED: To provide a program controller and a program controlling method capable of effectively establishing security in carrying out a program and to provide a program. SOLUTION: A controlling part 300 in an IC chip 200 mounted on an IC card 100 performs a security program recorded in an OS part 420 when initialized. In a DF area part 440, a plurality of kinds of programs for realizing a plurality of kinds of services are recorded in a plurality of areas. When an area corresponding to a desired service is designated, the controlling part 300 sets a hardware firewall (HWFW) in the corresponding area on the basis of the operation of the security program. The HWFW inhibits designation of another service during the performance of the program of the designated service and inhibits the program in execution from performing a program of another service.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－351567
（P2002－351567A）
(43)公開日　平成14年12月6日(2002.12.6)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　1/00 | | Ｂ４２Ｄ　15/10 | ５２１ | ２Ｃ００５ |
| Ｂ４２Ｄ　15/10 | ５２１ | Ｇ０６Ｆ　9/06 | ６６０Ｇ | ５Ｂ０３５ |
| Ｇ０６Ｋ　19/073 | | Ｇ０６Ｋ　19/00 | Ｐ | ５Ｂ０７６ |

審査請求　有　　請求項の数９　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－159183(P2001－159183)

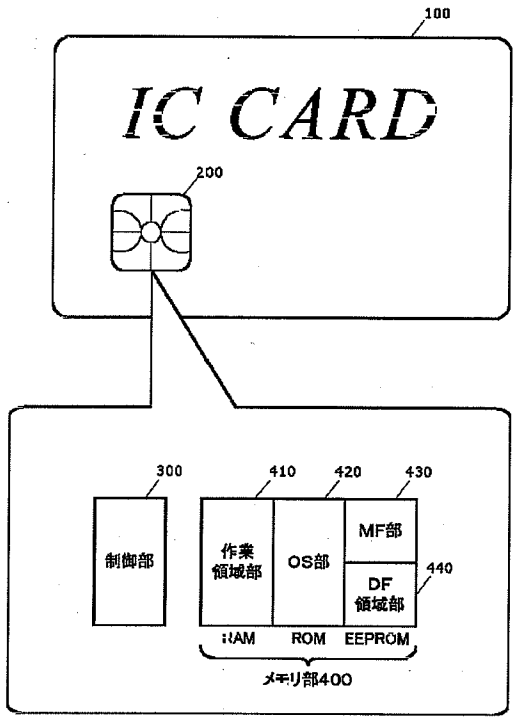
(22)出願日　平成13年５月28日(2001.5.28)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　七尾　慎司
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　竹内　隆
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095407
弁理士　木村　満

最終頁に続く

(54)【発明の名称】　プログラム制御装置および方法、ならびにプログラム

(57)【要約】
【課題】　プログラム実行時の安全性を効果的に確立することができるプログラム制御装置および方法、ならびにプログラムを提供することを目的とする。
【解決手段】　ＩＣカード１００に実装されているＩＣチップ２００内の制御部３００は、イニシャライズ時にＯＳ部４２０に記録されているセキュリティプログラムを実行する。ＤＦ領域部４４０には、複数種類のサービスを実現するための複数種類のプログラムが複数の領域に記録されている。所望のサービスに対応する領域が指定されると、セキュリティプログラムの動作に基づいて、制御部３００は当該領域に対してハードウェアファイアウォール（ＨＷＦＷ）を設定する。ＨＷＦＷにより、指定されたサービスのプログラム実行中は、他のサービスの指定、および、実行中のプログラムが他のサービスのプログラムを実行することが禁止される。



【特許請求の範囲】
【請求項１】複数の記憶領域を有する記録媒体に記録されている複数のプログラムの実行を制御するためのプログラム制御装置であり、
所定のサービスを実現するための少なくとも１つのプログラムを、前記複数の記憶領域のいずれか１つに割り当てるプログラム割当手段と、
実行するサービスを指定するサービス指定手段と、
前記サービス指定手段が指定したサービスを実現するプログラムを実行するプログラム実行手段と、
前記サービス指定手段がサービスを指定したことを契機に、前記サービス指定手段および前記プログラム実行手段を制御し、前記プログラム実行手段が同時に実行できるプログラムを、前記サービス指定手段が指定したサービスに対応するプログラムが割り当てられた記憶領域に記録されているプログラムに制限する実行制限手段と、
を備える、ことを特徴とするプログラム制御装置。
【請求項２】前記サービス指定手段は、指定したサービスに対応する記憶領域内のディレクトリを指定し、
前記実行制限手段は、前記サービス指定手段が指定したディレクトリに属するプログラムのみが実行されるよう、前記プログラム実行手段を制御する、
ことを特徴とする請求項１に記載のプログラム制御装置。
【請求項３】前記実行制限手段は、
前記プログラム実行手段がプログラムを実行している間、前記サービス指定手段が他のサービスを指定することを禁止する指定制限手段と、
前記プログラム実行手段が実行しているプログラムが他の記憶領域へのアクセスを要求しても、前記プログラム実行手段が他の記憶領域へアクセスすることを禁止するアクセス制限手段と、
を備える、ことを特徴とする請求項１または２に記載のプログラム制御装置。
【請求項４】前記記憶媒体はＩＣカードのプログラム記憶領域であり、
前記プログラム制御装置は前記ＩＣカードに実装されている、ことを特徴とする請求項１乃至３のいずれか１項に記載のプログラム制御装置。
【請求項５】複数の記憶領域を有する記録媒体に記録されている複数のプログラムの実行を制御するためのプログラム制御方法であり、
所定のサービスを実現するための少なくとも１つのプログラムを、前記複数の記憶領域のいずれか１つに割り当てるプログラム割当ステップと、
実行するサービスを指定するサービス指定ステップと、
前記サービス指定ステップで指定されたサービスを実現するためのプログラムを実行するプログラム実行ステップと、
前記サービス指定ステップでサービスが指定されたことを契機に、前記プログラム実行ステップで同時に実行されるプログラムを、前記サービス指定ステップで指定されたサービスに対応する記憶領域に記録されているプログラムに制限する実行制限ステップと、
を備える、ことを特徴とするプログラム制御方法。
【請求項６】前記サービス指定ステップでは、指定したサービスに対応するプログラムが割り当てられている記憶領域内のディレクトリが指定され、
前記実行制限ステップは、前記プログラム実行ステップで実行されるプログラムが、前記サービス指定ステップで指定されたディレクトリに属するプログラムのみとなるよう制限する、
ことを特徴とする請求項５に記載のプログラム制御方法。
【請求項７】前記実行制限ステップは、
前記プログラム実行ステップでプログラムが実行されている間、前記サービス指定ステップによる他のサービスの指定を禁止する指定制限ステップと、
前記プログラム実行ステップで実行されているプログラムが、他の記憶領域へのアクセスを要求しても、該他の記憶領域がアクセスされることを禁止するアクセス制限ステップと、
を備える、ことを特徴とする請求項５または６に記載のプログラム制御方法。
【請求項８】前記記憶媒体はＩＣカードのプログラム記憶領域である、ことを特徴とする請求項５乃至７のいずれか１項に記載のプログラム制御方法。
【請求項９】コンピュータを、請求項１乃至４のいずれか１項に記載のプログラム制御装置として機能させるプログラム。
【発明の詳細な説明】
【０００１】
【発明が属する技術分野】本発明は、プログラム制御装置および方法、ならびにプログラムに関し、特に、ＩＣカードに記録されたプログラムの実行に好適なプログラム制御装置および方法、ならびにプログラムに関する。
【０００２】
【従来の技術】集積回路（ＩＣチップ（ＩＣ：Integrated Circuit））を実装したＩＣカード（スマートカード）が普及しつつある。ＩＣカードは集積回路を実装しているため、従来の磁気カードなどに比べて記憶容量が圧倒的に大きいことに加え、自らプログラムを実行することができるので、広範囲な利用用途が期待されている。特に、複数のアプリケーションプログラムを記録し、それぞれをＩＣカード自身で実行することができるので、１枚のＩＣカードで複数種類のサービスの利用が可能となる、いわゆるマルチアプリケーション（マルチサービス）の用途に有用である。
【０００３】つまり、１枚のＩＣカードを、ＩＤカード、クレジットカード、キャッシュカード、電子財布

（電子マネー）、各種会員カード、ポイントカード、電子キー、電子チケット、などといった種々の用途に用いることができる。このような複数種類のサービス利用を実現するため、ＩＣカードには通常、使用者の用途に応じたアプリケーションプログラムを動的に記録・更新できる機能が備えられている。アプリケーションプログラムを動的に記録・更新できることで、使用者は所望する用途に応じたサービスの利用ができる反面、不正なプログラムを記録・実行することによる不正使用の可能性も高くなる。

【０００４】このような問題に対処するため、ＩＣカードにハードウェアファイアウォール（Hardware Firewal l、以下「ＨＷＦＷ」と称す）を実装したものも存在する。このＨＷＦＷは、各プログラムがアクセスできるメモリ領域を制限することで、他のサービスにかかるプログラムやデータの実行、読み出し、書き込みを制御し、不正実行を防止する。

【０００５】しかし、従来のＨＷＦＷの場合、制限されたメモリ領域にプログラムがアクセスしていないかを常に監視する必要があるため、各プログラムを常に実行可能な状態にしておく必要があった。このため、あるプログラム内に他のプログラムへジャンプするコマンド存在しそれが実行された場合、すべてのプログラムが実行可能状態にあるため、他のプログラムへのジャンプが実行され、不正使用がなされてしまう可能性があった。

【０００６】また、アクセスを制限するメモリ領域をプログラム毎に予め設定（固定的に設定）する必要があるので、一度設定した後に、新たなアプリケーションプログラムを記録した場合、そのプログラムに対してはファイアウォールは有効とはならない。このため、追加・更新したプログラムに対して安全性を確立することができず、複数種類のプログラムを記録することで種々のサービスが利用できるＩＣカードの利点を阻害してしまうという問題があった。

【０００７】

【発明が解決しようとする課題】本発明は、上記実状に鑑みてなされたもので、プログラム実行時の安全性を効果的に確立することができるプログラム制御装置および方法、ならびにプログラムを提供することを目的とする。

【０００８】

【課題を解決するための手段】上記目的を達成するため、本発明の第１の観点にかかるプログラム制御装置は、複数の記憶領域を有する記録媒体に記録されている複数のプログラムの実行を制御するためのプログラム制御装置であり、所定のサービスを実現するための少なくとも１つのプログラムを、前記複数の記憶領域のいずれか１つに割り当てるプログラム割当手段と、実行するサービスを指定するサービス指定手段と、前記サービス指定手段が指定したサービスを実現するプログラムを実行するプログラム実行手段と、前記サービス指定手段がサービスを指定したことを契機に、前記サービス指定手段および前記プログラム実行手段を制御し、前記プログラム実行手段が同時に実行できるプログラムを、前記サービス指定手段が指定したサービスに対応するプログラムが割り当てられた記憶領域に記録されているプログラムに制限する実行制限手段と、を備える、ことを特徴とする。

【０００９】上記プログラム制御装置において、前記サービス指定手段は、指定したサービスに対応する記憶領域内のディレクトリを指定し、前記実行制限手段は、前記サービス指定手段が指定したディレクトリに属するプログラムのみが実行されるよう、前記プログラム実行手段を制御することが望ましい。

【００１０】上記プログラム制御装置において、前記実行制限手段は、前記プログラム実行手段がプログラムを実行している間、前記サービス指定手段が他のサービスを指定することを禁止する指定制限手段と、前記プログラム実行手段が実行しているプログラムが他の記憶領域へのアクセスを要求しても、前記プログラム実行手段が他の記憶領域へアクセスすることを禁止するアクセス制限手段と、を備えることが望ましい。

【００１１】上記プログラム制御装置において、前記記憶媒体はＩＣカードのプログラム記憶領域であり、前記プログラム制御装置は前記ＩＣカードに実装されているものとすることができる。

【００１２】上記のような構成によれば、例えば、ＩＣカードなどの記録媒体に複数種類のサービスを実現するための複数種類のプログラムが記録されている場合、例えば、サービスを利用するためのホスト端末などからの指示に基づいて、ＩＣカードが実現できるサービスのいずれかが指定されたことを契機に、実行可能なプログラムが、指定されたサービスに割り当てられた記録領域内のプログラムに制限される。つまり、サービスの指定を契機に（動的に）、対象記憶領域にいわゆるハードウェアファイアウォール（ＨＷＦＷ）が設定される。これにより、予めＨＷＦＷを固定的に設定する場合と異なり、常にすべてのプログラムを実行可能状態にしておく必要がない。このため、実行中のプログラムが他のサービスのプログラムを実行してしまう事態を防止することができ、プログラム実行時の安全性を向上させることができる。さらに、予め制限対象のメモリ領域を設定しておく必要がないので、アプリケーションプログラムをインストールする記憶領域の自由度を高くすることができ、インストールするプログラムの数や容量に柔軟に対応することができる。

【００１３】この場合、例えば、指定された記憶領域にディレクトリが設定されている場合、サービス指定手段は、所望するプログラムを直下に含んだディレクトリを指定し、実行制御手段は、指定されたディレクトリ直下

のプログラムのみが実行されるよう、プログラム実行手段を制御する。これにより、所定のサービスを実現するためのプログラムのみが実行される。

【００１４】さらに、サービスの指定を契機に設定されたＨＷＦＷにより、所定のサービスのためのプログラムが実行されている間、サービス指定手段が他のサービスを指定することを禁止する。また、実行中のプログラムが、他のサービスにかかるプログラムの実行を要求しても、その実行は禁止される。これにより、所定のサービスにかかるプログラムのみが実行されるので、プログラム実行時の安全性を向上させることができる。

【００１５】上記目的を達成するため、本発明の第２の観点にかかるプログラム制御方法は、複数の記憶領域を有する記録媒体に記録されている複数のプログラムの実行を制御するためのプログラム制御方法であり、所定のサービスを実現するための少なくとも１つのプログラムを、前記複数の記憶領域のいずれか１つに割り当てるプログラム割当ステップと、実行するサービスを指定するサービス指定ステップと、前記サービス指定ステップで指定されたサービスを実現するためのプログラムを実行するプログラム実行ステップと、前記サービス指定ステップでサービスが指定されたことを契機に、前記プログラム実行ステップで同時に実行されるプログラムを、前記サービス指定ステップで指定されたサービスに対応する記憶領域に記録されているプログラムに制限する実行制限ステップと、を備える、ことを特徴とする。

【００１６】上記プログラム制御方法において、前記サービス指定ステップでは、指定したサービスに対応するプログラムが割り当てられている記憶領域内のディレクトリが指定され、前記実行制限ステップは、前記プログラム実行ステップで実行されるプログラムが、前記サービス指定ステップで指定されたディレクトリに属するプログラムのみとなるよう制限することが望ましい。

【００１７】上記プログラム制御方法において、前記実行制限ステップは、前記プログラム実行ステップでプログラムが実行されている間、前記サービス指定ステップによる他のサービスの指定を禁止する指定制限ステップと、前記プログラム実行ステップで実行されているプログラムが、他の記憶領域へのアクセスを要求しても、該他の記憶領域がアクセスされることを禁止するアクセス制限ステップと、を備えることが望ましい。

【００１８】上記プログラム制御方法において、前記記憶媒体はＩＣカードのプログラム記憶領域であるものとすることができる。

【００１９】上記目的を達成するため、本発明の第３の観点にかかるプログラムは、コンピュータを、上記プログラム制御装置として機能させることを特徴とする。

【００２０】

【発明の実施の形態】以下、図面を参照して本発明にかかる実施の形態を説明する。

【００２１】図１は本発明の実施の形態にかかるＩＣカード（スマートカード）の構成を説明するための図である。図示するようにＩＣカード１００には、ＩＣチップ２００が実装されている。同図下段は、ＩＣチップ２００の構成を模式的に示している。図示するように、ＩＣチップ２００は、制御部３００およびメモリ部４００を備えている。メモリ部４００はさらに、作業領域部４１０、ＯＳ部４２０、ＭＦ部４３０およびＤＦ領域部４４０を備えている。

【００２２】制御部３００は、例えば、ＣＰＵ（Central Processing Unit：中央演算処理装置）などから構成され、ＩＣカード１００を利用するためのホスト端末（不図示）からの指示（コマンド）に基づいてメモリ部４００を制御し、プログラムおよびデータの読み出し、書き込みおよび実行を行う。

【００２３】作業領域部４１０は、例えばＲＡＭ（Random Access Memory）などの読み書き可能な半導体記憶装置から構成され、制御部３００がプログラムを実行する際のワークエリアとして用いられる。

【００２４】ＯＳ（Operating System：基本ソフトウェア）部４２０は、例えばＲＯＭ（Read Only Memory）などの読み出し専用の半導体記憶装置から構成され、制御部３００が動作するための基本ソフトウェア（ＯＳ）などを記憶する。制御部３００は、ＯＳ部４２０に記録されているＯＳを実行することにより、ＩＣカード１００の各部を制御し、後述する各処理を実現する。

【００２５】また、このＯＳ部４２０には、制御部３００が後述するＤＦ領域部４４０に記録されているアプリケーションプログラムを実行する際のセキュリティ動作を行うセキュリティプログラムが記録されているものとする。本実施の形態にかかるハードウェアファイアウォール（ＨＷＦＷ）機能（後述）の動作は、制御部３００がセキュリティプログラムを実行することで実現される。

【００２６】このＯＳ部４２０に記録される各プログラムは、ＩＣチップ２００の製造時に記録されるものである。

【００２７】ＭＦ（Master File：マスタファイル）部４３０は、例えばＥＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory）などの書換可能な不揮発性半導体記憶装置から構成され、後述するＤＦ領域部４４０の根幹となるディレクトリ（以下、「ＭＦディレクトリ」と称す）が作成される。このＭＦディレクトリは、ＩＣカード１００がイニシャライズされた場合のカレントディレクトリとして設定されるものである。

【００２８】また、ＭＦ部４３０のＭＦディレクトリ直下には、後述するＤＦ領域部４４０に記録されている各プログラム（アプリケーションプログラム）が共通に実行可能な共通プログラムが格納されている。この共通プログラムは、動的に追加・更新可能（ダウンロード可

能）であり、MFディレクトリ直下に共通プログラムがダウンロードされた場合には、DF領域部４４０内の各アプリケーションプログラムによる実行が可能となる。

【００２９】なお、本実施の形態では、OS部４２０に記録されているセキュリティプログラムのサブプログラムが共通プログラムとしてMF部４３０に記録されるものとする。これは、セキュリティプログラムはICカード１００の初回使用時から実行されるべき重要なプログラムであるため、ICカード１００の発行時（より詳細にはICチップ２００の製造時）にOS部４２０に記録されるが、カード発行後にセキュリティプログラムの脆弱性が判明する場合がある。これに対処するため、追加・更新可能なMF部４３０に、セキュリティプログラムのサブプログラムやデータを動的に記録（ダウンロード）するようにし、常に最新のセキュリティ環境を実現できるようにする。つまり、後述するHWFWの動作は、OS部４２０のセキュリティプログラムとMF部４３０のサブプログラムとの協働により実現されるものである。

【００３０】DF（Dedicated File：専用ファイル）領域部４４０は、例えばEEPROM（Electrically Erasable Programmable Read-Only Memory）などの書換可能な不揮発性半導体記憶装置から構成され、ICカード１００を利用した複数種類のサービスを実現するためのプログラム（アプリケーションプログラム）やデータが格納される。DF領域部４４０はさらに、図2に示すようにサービス毎に記憶領域が分割される。本実施の形態では、ICカード１００で利用できるサービスをサービス1～サービスn（例えば、サービス1は「電子財布」、サービス2は「IDカード」、サービスnは「電子キー」とする）とし、DF領域部４４０は、各サービスに対応したサービス別領域４４０－1～４４０－nを有するものとする。

【００３１】図3は、MF部４３０とDF領域部４４０との関係を模式的に示した図である。図示するように、DF領域部４４０の各サービス別領域４４０－1～４４０－nには、それぞれのサービスに必要となるプログラムファイル、データファイルなどが格納されている。また、各サービス別領域４４０－1～４４０－nには、必要に応じてさらにディレクトリが用意され、それぞれのディレクトリにプログラムファイルやデータファイルが格納されている。

【００３２】次に、図4のフローチャートを参照して、本実施の形態にかかるICカード１００のプログラム実行処理を説明する。

【００３３】まず、ICカード１００が、所望するサービスを提供するホスト端末（不図示）に装着されるなどして、ICカード１００とホスト端末との交信が開始されると（ステップS１０１：Yes）、ホスト端末はICカード１００に対しイニシャライズ用のコマンドを発行する。

【００３４】ICカード１００の制御部３００は、ホスト端末からイニシャライズ用コマンドを受信すると、OS部４２０のOSおよびセキュリティプログラムが実行される（ステップS１０２）。

【００３５】ステップS１０２で実行されたOSの動作に基づいて、制御部３００は、図5（a）に示すように、MF部４３０のMFディレクトリをカレントディレクトリとして設定する（ステップS１０３）。MFディレクトリがカレントディレクトリとなることで、MFディレクトリ直下の共通プログラム、つまり、セキュリティサブプログラムが実行可能状態となる。このセキュリティサブプログラムは、ステップS１０２で起動されたセキュリティプログラムの指示により実行されるものとする。なお、図5，６，８において、実行中あるいは実行可能状態のプログラムを反転表示にて示すものとする。

【００３６】次に、ホスト端末から、当該ホスト端末が提供するサービスを指定するコマンドがICカード１００に送信されると（ステップS１０４：Yes）、制御部３００は、当該サービスに対応するサービス別領域４４０－1～４４０－nのルートディレクトリをカレントディレクトリに設定する（ステップS１０５）。ここでは、サービス1が指定された場合を例に説明する。

【００３７】ステップS１０２およびS１０３で起動されたセキュリティプログラムの動作に基づいて、制御部３００は、ステップS１０５でルートディレクトリをカレントディレクトリに設定したことを契機に、当該ルートディレクトリに対応するサービス別領域４４０－1にハードウェアファイアウォール（Hardware Firewall、以下「HWFW」と称す）を設定する（ステップS１０６、図5（b））。つまり、HWFWを動的に設定する。ここで、サービス1のルートディレクトリの下にはディレクトリが存在していないため（ステップS１０７：No）、同図にて反転表示で示すように、ルートディレクトリ直下のプログラムが実行可能状態となる。つまり、カレントディレクトリの直下に属するプログラムのみが実行可能状態となる（ステップS１０９）。

【００３８】一方、サービス別領域４４０－1～４４０－n内に、複数のディレクトリが存在する場合（サービス2の例）は、セキュリティプログラムの動作に基づいて、サービス2の指定、つまりルートディレクトリが指定されたこと（ステップS１０５）を契機に、制御部３００はサービス2に対応するサービス別領域４４０－2にHWFWを設定する（ステップS１０６、図6（a））。

【００３９】ホスト端末が、必要なプログラムが格納されているディレクトリ（同図中ディレクトリ1）を指定すると（ステップS１０７：Yes）、図6（b）にて反転表示で示すように、ディレクトリ1直下のプログラ

ムが実行可能状態となる。つまり、カレントディレクトリの直下に属するプログラムのみが実行可能状態となる。

【００４０】そして、制御部３００が、実行可能状態となったプログラムを実行する。つまり、ステップＳ１０７にてディレクトリの指定があった場合には（ステップＳ１０７：Ｙｅｓ）、当該ディレクトリ直下のプログラムが実行され（ステップＳ１０８）、ルートディレクトリ以外のディレクトリが存在しないサービスが選択された場合（ステップＳ１０７：Ｎｏ）は、ルートディレクトリ直下のプログラムが実行される（ステップＳ１０９）。

【００４１】ステップＳ１０８またはＳ１０９にてプログラムが実行されると、ステップＳ１０６で設定されたＨＷＦＷにより、実行されているプログラムの動作が監視される（ステップＳ２００）。

【００４２】このＨＷＦＷによるプログラム監視処理を、図７のフローチャートを参照して説明する。ここでは、図６（ｂ）に示すように、サービス別領域４４０－２（サービス２）のディレクトリ１に属するプログラムが実行されている場合を例に説明する。

【００４３】まず、図８（ａ）に示すように、サービス別領域４４０－２のディレクトリ１に属するプログラム（図中、反転表示）が実行されている間に、ホスト端末からのコマンドによりサービスｎが指定されても、つまり、サービス別領域４４０－ｎのルートディレクトリにカレントが設定されても（ステップＳ２０１：Ｙｅｓ）、制御部３００は、セキュリティプログラムの動作に基づいて、このカレントが設定されたルートディレクトリ（さらなるディレクトリが存在する場合は、指定されたディレクトリ）に属するプログラムの実行を許可しない（ステップＳ２０２）。

【００４４】一方、図８（ｂ）に示すように、現在実行しているサービス２のプログラム（図中、反転表示）が、サービス別領域４４０－１のプログラムの実行を要求した場合（ステップＳ２０３：Ｙｅｓ、Ｓ２０４：Ｙｅｓ）、制御部３００は、セキュリティプログラムの動作に基づいて、要求されたプログラム（図中、サービス別領域４４０－１内、ルートディレクトリ直下のプログラム）の実行を許可しない（ステップＳ２０５）。また、この場合、例えば実行中のサービス２のプログラムが、サービス別領域４４０－１内のデータファイルからデータの取得を要求しても、制御部３００はこれを許可しない。

【００４５】しかし、実行中のサービス２のプログラムが、サービス別領域４４０－２のディレクトリ２に属するプログラム（不図示）の実行やデータファイル（不図示）からデータの取得を要求した場合（ステップＳ２０３：Ｙｅｓ、Ｓ２０４：Ｎｏ）は、ＨＷＦＷが設定されているサービス別領域４４０－２内であるのでこれを許可する（ステップＳ２０６）。

【００４６】アプリケーションプログラム実行中は、制御部３００がステップＳ２０１～Ｓ２０６の処理を常に行い、アプリケーションプログラムの動作を監視する（ステップＳ２０７：Ｎｏ）。

【００４７】当該アプリケーションプログラムの実行が終了すると（ステップＳ２０７：Ｙｅｓ）、制御部３００は、カレントディレクトリを、サービス別領域４４０－２のディレクトリ１からＭＦディレクトリに変更設定する（ステップＳ２０８）。

【００４８】ステップＳ２０８でＭＦディレクトリがカレントディレクトリとなったことを契機に、制御部３００は、セキュリティプログラムの動作に基づいて、サービス別領域４４０－２に設定していたＨＷＦＷを解除して（ステップＳ２０９）、図４に示すプログラム実行処理に戻り、処理を終了する。

【００４９】以上説明したように、本発明にかかる実施の形態によれば、複数のサービスを実現するＩＣカード１００で実行されるプログラムに対して、サービス指定時に動的にＨＷＦＷ設定を設定するので、予め監視対象のメモリ領域を設定することでＨＷＦＷを固定的に設定する場合と異なり、ＤＦ領域部４４０へのプログラム（アプリケーションプログラム）やデータの追加・更新により自由度を持たせることができ、複数種類のプログラムを記録することで複数種類のサービスの利用を実現するＩＣカードの利便性を有効に活用することができる。

【００５０】また、本実施の形態で設定されるＨＷＦＷは、あるプログラムが実行されている間に他のサービスが指定されることを禁止するとともに、実行されているプログラムが他のサービスのプログラム（他のサービス別領域４４０に記録されているプログラム）を実行することを禁止するので、不正なプログラムを記録・実行することによる不正動作を防止することができる。

【００５１】上記実施の形態では、本発明をＣＰＵ（制御部３００）を実装するＩＣカード１００に適用した例を説明したが、本発明が適用可能な記録媒体はこれに限られない。例えば、ＣＰＵを実装しないＩＣカード（メモリカード）に記録された複数のプログラムをホスト端末が実行する形態に本発明を適用してもよい。さらにこの場合、ホスト端末は専用装置に限られず、例えばパーソナルコンピュータなどの通常のコンピュータシステムを利用してもよい。この場合、上述の処理を実現するプログラムをコンピュータにインストールして実行することで、上述の制御部３００の動作と同様の動作を実現することができる。

【００５２】ここで、コンピュータにプログラムを供給する方法は任意である。例えば、上記プログラムを記録した媒体（例えば、フレキシブルディスク、ＣＤ－ＲＯＭ（Compact Disc Read-Only Memory）、ＤＶＤ(Digita

l Versatile Disk)など）からインストールしてもよく、または、例えば通信回線、通信ネットワーク、通信システムなどを介して供給してもよい。この場合、例えば、通信ネットワークの掲示板（ＢＢＳ：Bulletin Board System）に当該プログラムを掲示し、これをネットワークを介して搬送波に重畳してコンピュータに配信する。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケーションプログラムと同様に実行することで、上述の処理を実行することができる。

【００５３】

【発明の効果】以上説明したように、本発明によれば、プログラム実行時の安全性を効果的に確立することができるプログラム制御装置および方法、ならびにプログラムを提供することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態にかかるＩＣカードの外観と、ＩＣカードのＩＣチップ内の構成を説明するための図である。

【図２】図１に示すＤＦ領域部の詳細を説明するための図である。

【図３】図１に示すＭＦ部とＤＦ領域部との関係を説明するための図である。

【図４】本発明の実施の形態にかかるプログラム実行処理を説明するためのフローチャートである。

【図５】図４に示す処理の例を説明するための図であり、（ａ）は共通プログラムの実行時の処理を説明するための図であり、（ｂ）は、所定のサービスのルートディレクトリが指定された場合の処理を説明するための図である。

【図６】図４に示す処理の他の例を説明するための図であり、（ａ）は他のサービスのルートディレクトリが指定された場合の処理を説明するための図であり、（ｂ）は、サービス別領域内のディレクトリが指定された場合の処理を説明するための図である。

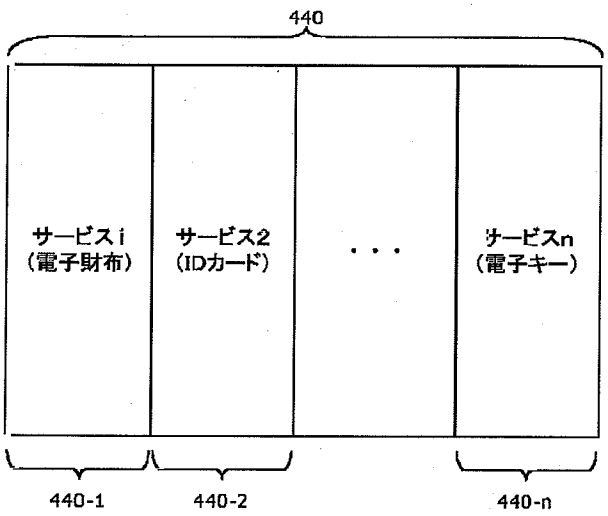
【図７】図４に示すＨＷＦＷによる監視処理を説明するためのフローチャートである。

【図８】図７に示す処理の例を説明するための図であり、（ａ）はプログラム実行時に他のサービスが指定された場合の処理を説明するための図であり、（ｂ）は実行中のプログラムが、他のサービスのプログラムやデータを指定した場合の処理を説明するための図である。

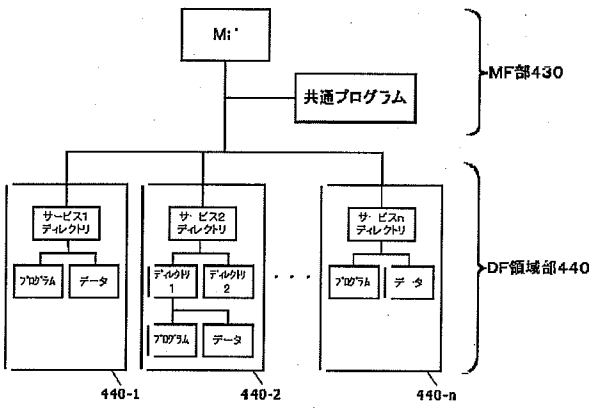
【符号の説明】

１００　ＩＣカード
２００　ＩＣチップ
３００　制御部
４００　メモリ部
４１０　作業領域部
４２０　ＯＳ（Operation System）部
４３０　ＭＦ（Master File）部
４４０　ＤＦ（Dedicated File）領域部

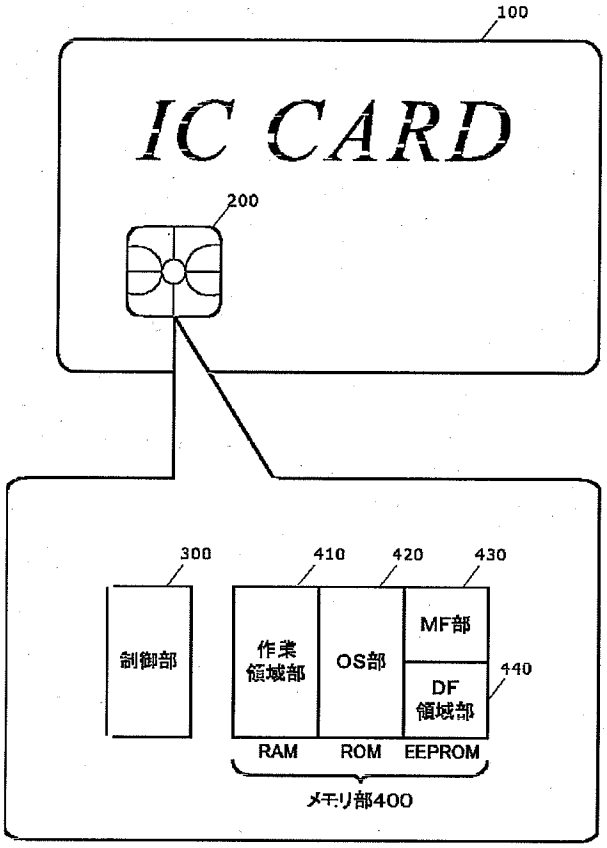
【図２】



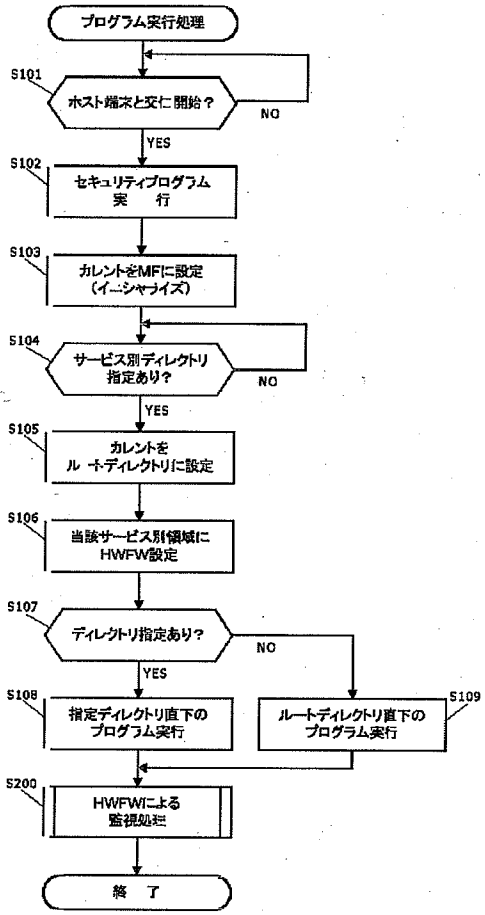

【図３】



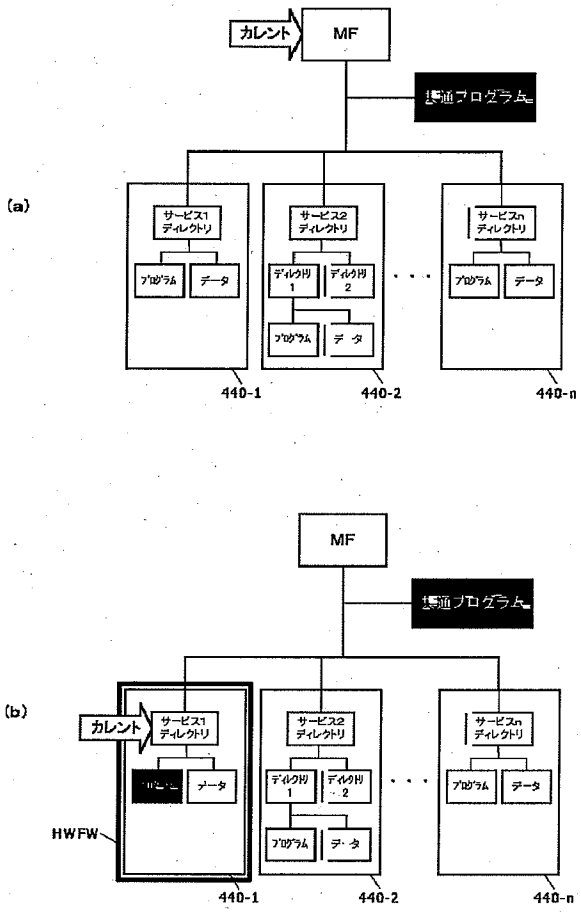
【図1】


100
IC CARD
200
300
410
420
430
制御部
作業領域部
OS部
MF部
DF領域部
440
RAM
ROM
EEPROM
メモリ部400

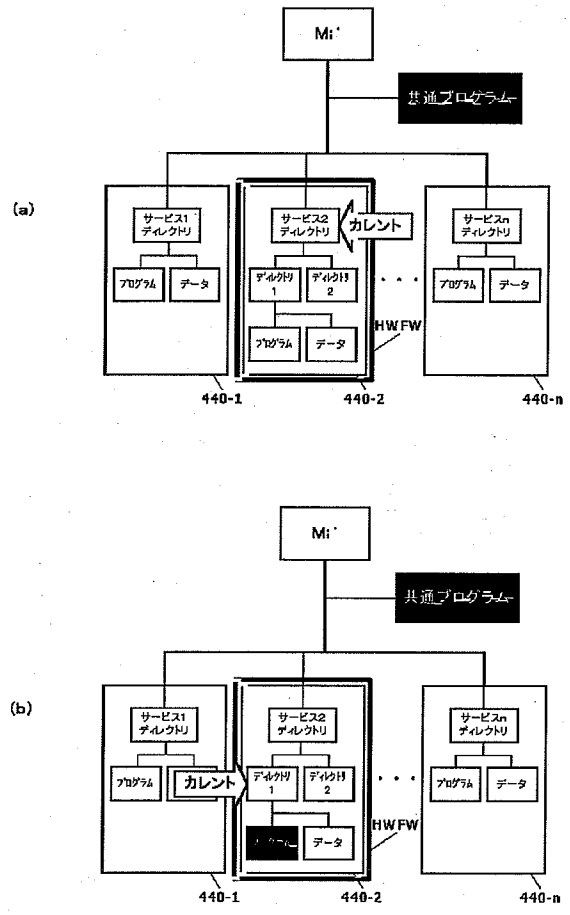
【図4】


プログラム実行処理
S101
ホスト端末と交信開始？
NO
YES
S102
セキュリティプログラム実行
S103
カレントをMFに設定（イニシャライズ）
S104
サービス別ディレクトリ指定あり？
NO
YES
S105
カレントをルートディレクトリに設定
S106
当該サービス別領域にHWFW設定
S107
ディレクトリ指定あり？
NO
YES
S108
指定ディレクトリ直下のプログラム実行
S109
ルートディレクトリ直下のプログラム実行
S200
HWFWによる監視処理
終了

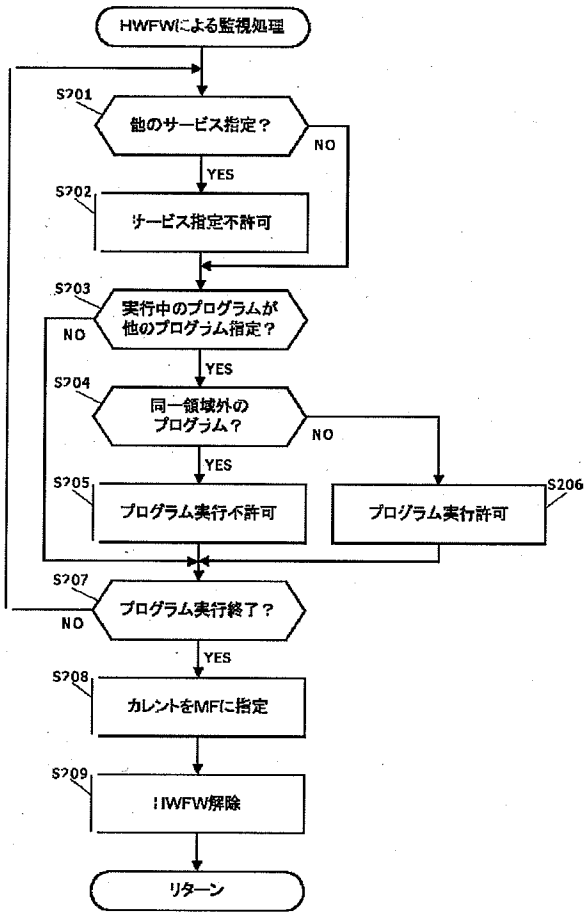
【図5】


(a)
カレント
MF
共通プログラム
サービス1 ディレクトリ
サービス2 ディレクトリ
サービスn ディレクトリ
プログラム
データ
ディレクトリ 1
ディレクトリ 2
440-1
440-2
440-n
(b)
HWFW

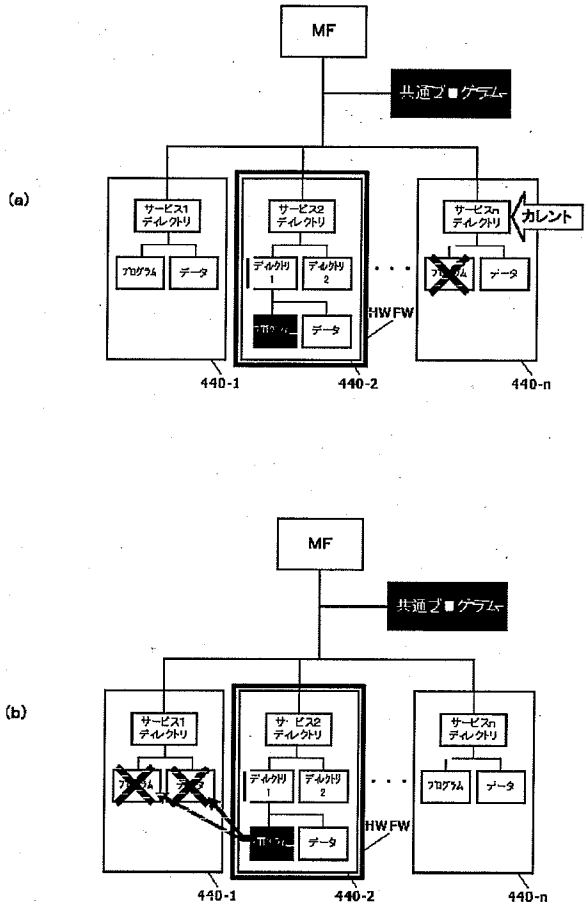
【図6】


(a)
Mi
共通プログラム
サービス1 ディレクトリ
サービス2 ディレクトリ
サービスn ディレクトリ
カレント
プログラム
データ
ディレクトリ 1
ディレクトリ 2
HWFW
440-1
440-2
440-n
(b)

【図7】




【図8】




フロントページの続き

(72)発明者　市原　尚久
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

(72)発明者　山本　真也
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

Ｆターム(参考)　2C005 MA01 MB05 SA22 SA25
5B035 AA13 BB09 CA11 CA38
5B076 FB01 FB02 FB03